UNITED
STATES
SIGNALS
INTELLIGENCE
DIRECTIVE

USSID SP0018

(U) LEGAL COMPLIANCE AND U.S. PERSONS MINIMIZATION PROCEDURES

ISSUE DATE: 25 January 2011

REVISED DATE:

(U) OFFICE OF PRIMARY CONCERN (OPC)

National Security Agency/Central Security Service (NSA/CSS), Signals Intelligence Directorate (SID), Office of General Counsel

---

(U) LETTER OF PROMULGATION, ADMINISTRATION, AND AUTHORIZATION

(U) Topic of Promulgation

(U) USSID SP0018 prescribes policies and procedures and assigns responsibilities to ensure that the missions and functions of the United States SIGINT System (USSS) are conducted in a manner that safeguards the constitutional rights of U.S. persons. This USSID delineates and promulgates the USSS minimization policy and procedures required to protect the privacy

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20370601

rights of **U.S. persons.**

(U) USSID Edition

(U) This USSID supersedes USSID SP0018, dated 27 July 1993, which must now be destroyed.

(U) Legal Protection of Sensitive Information

(U//~~FOUO~~) This USSID contains sensitive information that is legally protected from public disclosure and is to be used only for official purposes of National Security Agency/Central Security Services (NSA/CSS).

(U) Handling of USSID

(U//~~FOUO~~) Users must strictly adhere to all classification and handling restrictions (see NSA/CSS Classification Manual 1-52) when:

- (U) storing hard or soft copies of this USSID, or
- (U) hyperlinking to this USSID.

(U) Users are responsible for the update and management of this USSID when it is stored locally.

(U) Location of Official USSID

(U//~~FOUO~~) The SIGINT Policy System Manager will maintain and update the current official USSID on NSANet. As warranted, the USSID will be available on INTELINK.

(U) Access by Contractors and Consultants

(U) For NSA elements to include the SIGINT Extended Enterprise:

(U//~~FOUO~~) USSS contractors or consultants assigned to NSA/CSS Headquarters or to other elements of the SIGINT Extended Enterprise are pre-authorized for access to USSIDs via NSANet, Intelink, or in hard-copy formats as needed to perform their jobs. However, for those sensitive USSIDs for which access is password-controlled, all users, to include contractors, must undergo additional security and mission vetting.

(U) Outside NSA elements:

(U//~~FOUO~~) Non-USSS contractors or consultants working at external facilities are pre-authorized for soft-copy access to USSIDs via NSANet or in selected cases, via INTELINK, if connectivity to those systems is allowed by the contractor's NSA/CSS sponsor. Where such connectivity is not established, any hard-copy provision of USSIDs must be authorized by the SIGINT Policy System Manager (NSTS: 966-5487, STE: [redacted] DSN: [redacted]

(b)(3)-P.L. 86-36

(U) Access by Third Party

(U) This USSID is not releasable to any Third Party partner.

Partners

(U) If a shareable version of this USSID is requested:

- (U) refer to USSID SP0002, Annex B, and
- (U) contact the appropriate Country Desk Officer in the Foreign Affairs Directorate.

(U) Executive Agent

(U) The Executive Agent for this USSID is:

//s//
KEITH B. ALEXANDER
General, U. S. Army
Director, NSA/Chief, CSS

(U) TABLE OF CONTENTS

(U) Sections

(U) Annexes and Appendices

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

SECTION 1 - (U) PREFACE

(U) Fourth Amendment Protections

1.1. (U) The Fourth Amendment to the United States Constitution protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. Government. The Supreme Court has ruled that the interception of electronic communicatio ns is a search and seizure within the meaning of the Fourth Amendment. It is therefore mandatory that signals intelligence (SIGINT) operations be conducted pursuant to procedures which meet the reasonableness requirements of the Fourth Amendment.

(U) Balancing Foreign Intelligence Need and Privacy Interest

1.2. (U) In determining whether United States SIGINT System (USSS) operations are "reasonable," it is necessary to balance the U.S. Government's need for foreign intelligence information and the privacy interests of persons protected by the Fourth Amendment. Striking that balance has consumed much time and effort by all branches of the United States Government. The results of that effort are reflected in the references listed in Section 2 below. Together, these references require the minimization of U.S. person information collected, processed, retained or disseminated by the USSS. The purpose of this document

is to implement these minimization requirements.

1.3. (U) Several themes run throughout this USSID. The most important is that intelligence operations and the protection of constitutional rights are not incompatible. It is not necessary to deny legitimate foreign intelligence collection or suppress legitimate foreign intelligence information to protect the Fourth Amendment rights of U.S. persons.

(U) Minimization of U.S. Person Information

1.4. (U) These minimization procedures implement the constitutional principle of "reasonableness" by giving different categories of individuals and entities different levels of protection. These levels range from the stringent protection accorded U.S. citizens and permanent resident aliens in the United States to provisions relating to foreign diplomats in the U.S. These differences reflect yet another main theme of these procedures, that is, that the focus of all foreign intelligence operations is on foreign entities and persons.

(U) Oversight Functions

1.5. (U) Nothing in these procedures shall restrict the performance of lawful compliance or oversight functions over the USSS.

SECTION 2 - (U) REFERENCES

(U) References

2.1 (U) The following documents are references to this USSID:

- (U) 50 U.S.C. 1801, et seq., Foreign Intelligence Surveillance Act (FISA) of 1978, as amended.
- (U) Executive Order 12333, "United States Intelligence Activities," as amended 30 July 2008.
- (U) (U) DoD Directive 5240.01, "DoD Intelligence Activities," dated 27 August 2007.
- (U) NSA/CSS Policy No. 1-23, "Procedures Governing NSA/CSS Activities that affect U.S. Persons," as revised 29 May 2009.
- (U) DoD Regulation 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Person," dated December 1982.

SECTION 3 - (U) POLICY

(U) Policy and the USSS Foreign

3.1. (U) The policy of the USSS is to TARGET or COLLECT only FOREIGN COMMUNICATIONS.* The USSS will not intentionally COLLECT

Communications Mission

communications to, from or about U.S. PERSONS or persons or entities in the U.S. except as set forth in this USSID. If the USSS inadvertently COLLECTS such communications, it will process, retain and disseminate them only in accordance with this USSID.

* (U) Capitalized words in Sections 3 through 9 are defined terms in Section 9.

SECTION 4 - (U) COLLECTION

(U) Collection

4.1. ~~(S//SI//REL)~~ Communications which are known to be to, from or about a U.S. PERSON [redacted] not be intentionally intercepted, or selected through the use of a SELECTION TERM, except in the following instances: (b)(1)

a. (U//~~FOUO~~) With the approval of the United States Foreign Intelligence Surveillance Court either under the conditions outlined in Annex A of this USSID or as permitted by other FISA authorities.

b. (U) With the approval of the Attorney General of the United States, if:

(1) (U) The COLLECTION is directed against the following:

(a) (U//~~FOUO~~) Communications to or from U.S. PERSONS outside the UNITED STATES if such persons have been approved for targeting in accordance with the terms of FISA (e.g., the targeted U.S. PERSON is the subject of an order or authorization issued pursuant to Sections 105, 703, 704, or 705(b) of FISA), or

(b) ~~(S//SI//REL)~~ International communications to, from, [redacted] (b)(1)

(c) (U//~~FOUO~~) Communications which are not to or from but merely about U.S. PERSONS (wherever located).

(2) (U) The person is an AGENT OF A FOREIGN POWER, and

(3) (U) The purpose of the COLLECTION is to acquire significant FOREIGN INTELLIGENCE information.

c. (U//~~FOUO~~) With the approval of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), so long as the COLLECTION need not be approved by the Foreign Intelligence Surveillance Court or the Attorney General, and

(1) (U//FOUO) The person has CONSENTED to the COLLECTION by executing one of the CONSENT forms contained in Annex H, or

(2) (U//FOUO) The person is reasonably believed to be held captive by a FOREIGN POWER or group engaged in INTERNATIONAL TERRORISM, or

(3) (S//REL) The TARGETED [redacted] and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex I, or

(b)(1)

(4) (S//SI//REL) The COLLECTION is directed against [redacted] between a U.S. PERSON in the UNITED STATES and a foreign entity outside the UNITED STATES, the TARGET is the foreign entity, and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex K, or

(5) (S//SI//REL) Technical devices (e.g., [redacted] are employed to limit acquisition by the USSS to communications to or from the TARGET or to specific forms of communications used by the TARGET (e.g., [redacted] and the COLLECTION is directed against [redacted] voice and facsimile communications with one COMMUNICANT in the UNITED STATES, and the TARGET of the COLLECTION is [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

(a) A non-U.S. PERSON located outside the UNITED STATES, [redacted]

(b) [redacted]

(b)(1)

(6) (U//FOUO) Copies of approvals granted by the DIRNSA/CHCSS under these provisions will be retained in the Office of General Counsel for review by the Attorney General.

d. (U) Emergency Situations.

(1) (U//FOUO) Unless separate authorization under FISA is required by law,[1] in emergency situations DIRNSA/CHCSS may

1 (U//FOUO) Collection that constitutes "electronic surveillance" as defined by FISA can only be authorized in accordance with the terms of FISA. Under certain circumstances, the Attorney General may authorize emergency collection that constitutes "electronic surveillance" under FISA. For purposes of FISA, the term

authorize the COLLECTION of information to, from, or about a U.S. PERSON who is outside the UNITED STATES when securing the prior approval of the Attorney General is not practical because:

(a) (U) The time required to obtain such approval would result in the loss of significant FOREIGN INTELLIGENCE and would cause substantial harm to the national security.

(b) (U) A person's life or physical safety is reasonably believed to be in immediate danger.

(c) (U) The physical security of a defense installation or government property is reasonably believed to be in immediate danger.

(2) (U//~~FOUO~~) In those cases where the DIRNSA/CHCSS authorizes emergency COLLECTION, except for actions taken under paragraph d.(1)(b) above, DIRNSA/CHCSS shall find that there is probable cause that the TARGET meets one of the following criteria:

(a) (U) A person who, for or on behalf of a FOREIGN POWER, is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or INTERNATIONAL TERRORIST activities, or activities in preparation for INTERNATIONAL TERRORIST activities; or who conspires with, or knowingly aids and

---

"electronic surveillance" encompasses 1) the acquisition by an electronic, mechanical, or other surveillance device the contents of any wire or radio communications sent by or intended to be received by a particular, known, United States person if the contents are acquired by intentionally targeting the U.S. person under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, absent the U.S. person's express or implied consent; 2) the acquisition by electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18 of the United States Code; 3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required if the acquisition were undertaken for law enforcement purposes, and if both the sender and all intended recipients are located inside the United States; or 4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required if the acquisition were undertaken for law enforcement purposes.

abets a person engaging in such activities.

(b) (U) A person who is an officer or employee of a FOREIGN POWER.

(c) (U) A person unlawfully acting for, or pursuant to the direction of, a FOREIGN POWER. The mere fact that a person's activities may benefit or further the aims of a FOREIGN POWER is not enough to bring that person under this subsection, absent evidence that the person is taking direction from, or acting in knowing concert with, the FOREIGN POWER.

(d) (U) A CORPORATION or other entity that is owned or controlled directly or indirectly by a FOREIGN POWER.

(e) (U) A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access.

(3) (U) In all cases where emergency collection is authorized, the following steps shall be taken:

(a) (U//FOUO) The General Counsel will be notified immediately that the COLLECTION has started.

(b) (U//FOUO) The General Counsel will initiate immediate efforts to obtain Attorney General approval to continue the collection. If Attorney General approval is not obtained within 72 hours, the COLLECTION will be terminated. If the Attorney General approves the COLLECTION, it may continue for the period specified in the approval.

e. (U//FOUO) Annual reports to the Attorney General are required for COLLECTION conducted under paragraphs 4.1.c.(3) and (4). Responsible analytic offices will provide such reports through the Signals Intelligence Director and the General Counsel (GC) to the DIRNSA/CHCSS for transmittal to the Attorney General by 31 January of each year.

(U) [redacted] 4.2. ~~(S//SI//REL)~~ [redacted]

a. ~~(S//SI//REL)~~ [redacted]

(b)(1)

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

b. ~~(S//SI//REL)~~ [redacted]

(U) Incidental Acquisition of U.S. Person Information

4.3. (U) Information to, from or about U.S. PERSONS acquired incidentally as a result of COLLECTION directed against appropriate FOREIGN INTELLIGENCE TARGETS may be retained and processed in accordance with Section 5 and Section 6 of this USSID.

(U) Nonresident Alien Targets

4.4. ~~(S//SI//REL)~~ Nonresident Alien TARGETS Entering the UNITED STATES.

a. ~~(S//SI//REL)~~ If the communications of a nonresident alien located abroad are being TARGETED and the USSS learns that the individual has entered the UNITED STATES, COLLECTION may continue for a period of 72 hours provided that continued COLLECTION is otherwise permitted by FISA,2 the DIRNSA/CHCSS is advised immediately, and:

(1) Immediate efforts are initiated to obtain Attorney General approval, or

(2) A determination is made within the 72 hour period that the [redacted] (b)(1)

b. (U) If Attorney General approval is obtained, the COLLECTION may

---

2 ~~(S//SI//REL)~~ There is no 72 hour grace period for collection that has been authorized pursuant to Sections 702, 703, 704, or 705(b) of FISA. Collection under Sections 702, 703, 704, or 705(b) of FISA must be terminated as soon as the USSS learns the target has entered the United States. Similarly, DIRNSA may not authorize use of a collection technique while the target is located inside the United States if use of the collection technique would qualify as "electronic surveillance" under FISA (*see* Footnote 1).

continue for the length of time specified in the approval.

c. (U//~~FOUO~~) If it is determined that [redacted] COLLECTION may continue at the discretion of the operational element.

(b)(1)

d. (~~S//SI//REL~~) If [redacted] or if Attorney General approval is not obtained within 72 hours, COLLECTION must be terminated [redacted] Attorney General approval is obtained, or the individual leaves the UNITED STATES.

(U//~~FOUO~~) U.S. Person Targets

4.5. (U//~~FOUO~~) U.S. PERSON TARGETS Entering the UNITED STATES.

a. (U//~~FOUO~~) If communications to, from or about a U.S. PERSON located outside the UNITED STATES are being COLLECTED under Court or Attorney General approval as described in Sections 4.1.a. and 4.1.b. above, the COLLECTION must stop when the USSS learns that the individual has entered the UNITED STATES.

b. (U//~~FOUO~~) While the individual is in the UNITED STATES, COLLECTION may be resumed only with the approval of the United States Foreign Intelligence Surveillance Court as described in Annex A.

4.6. (~~S//REL~~) Requests to TARGET U.S. PERSONS. All proposals for COLLECTION against U.S. PERSONS, [redacted] must be submitted through the Signals Intelligence Director and the GC to the DIRNSA/CHCSS for review.

(b)(1)

(U) Direction Finding

4.7. (U//~~FOUO~~) Use of direction finding solely to determine the location of a transmitter located outside of the UNITED STATES does not constitute ELECTRONIC SURVEILLANCE or COLLECTION even if directed at transmitters believed to be used by U.S. PERSONS. Unless COLLECTION of the communications is otherwise authorized under these procedures, the contents of communications to which a U.S. PERSON is a party monitored in the course of direction finding may only be used to identify the transmitter.

(U) Distress Signals

4.8. (U) Distress signals may be intentionally collected, processed, retained, and disseminated without regard to the restrictions contained in this USSID.

(U) Automated Information Systems

4.9. (U) COMSEC Monitoring and Security Testing of Automated Information Systems. Monitoring for communications security purposes must be conducted with the consent of the person being monitored and in accordance with the

procedures established in National Telecommunications and Information Systems Security Directive 600, Communications Security (COMSEC) Monitoring, dated 10 April 1990. Monitoring for communications security purposes is not governed by this USSID. Intrusive security testing to assess security vulnerabilities in automated information systems likewise is not governed by this USSID.

SECTION 5- (U) PROCESSING

(U) Selection Terms 5.1. ~~(S//SI//REL)~~ Use of Selection Terms During Processing. When a SELECTION TERM is intended to INTERCEPT a communication on the basis of the content of the communication, or because a communication is enciphered, rather than on the basis of the identity of the COMMUNICANT or the fact that the communication mentions a particular individual, the following rules apply:

a. ~~(S//SI//REL)~~ No SELECTION TERM that is reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON (wherever located), [redacted] may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained by use of such SELECTION TERM. (b)(1)

b. (U//~~FOUO~~) No SELECTION TERM that has resulted in the INTERCEPTION of a significant number of communications to or from such persons or entities may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained.

c. (U//~~FOUO~~) SELECTION TERMS that have resulted or are reasonably likely to result in the INTERCEPTION of communications to or from such persons or entities shall be designed to defeat, to the greatest extent practicable under the circumstances, the INTERCEPTION of those communications which do not contain FOREIGN INTELLIGENCE.

5.2. (U//~~FOUO~~) Annual Review by the Signals Intelligence Director:

a. (U//~~FOUO~~) All SELECTION TERMS that are reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON or terms that have resulted in the INTERCEPTION of a significant number of such communications shall be reviewed annually by the Signals Intelligence Director or a designee.

b. (U//~~FOUO~~) The purpose of the review shall be to determine whether there is reason to believe that FOREIGN INTELLIGENCE will be obtained, or will continue to be obtained, by the use of these SELECTION TERMS.

c. (U//~~FOUO~~) A copy of the results of the review will be provided to the Inspector General (IG) and the GC.

(U) Intercepted Material

5.3. (U) Forwarding of Intercepted Material. FOREIGN COMMUNICATIONS collected by the USSS may be forwarded as intercepted to NSA, intermediate processing facilities, and collaborating centers.

5.4. (U) Non-foreign Communications.

a. (U) Communications between persons in the UNITED STATES. Private communications solely between persons in the UNITED STATES inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be promptly destroyed unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

b. (U) Communications between U.S. PERSONS. Communications solely between U.S. PERSONS will be treated as follows:

(1) (U) Communications solely between U.S. PERSONS inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be destroyed upon recognition, if technically possible, except as provided in paragraph 5.4.d. below.

(2) (U) Notwithstanding the preceding provision, cryptologic data (e.g., signal and encipherment information) and technical communications data (e.g., circuit usage) may be extracted and retained from those communications if necessary to:

(a) (U) Establish or maintain intercept, or

(b) (U) Minimize unwanted intercept, or

(c) (U) Support cryptologic operations related to FOREIGN COMMUNICATIONS.

c. (U) Communications Involving an Officer or Employee of the U.S. Government. Communications to or from any officer or employee of

the U.S. Government, or any state or local government, will not be intentionally intercepted. Inadvertent INTERCEPTIONS of such communications (including those between foreign TARGETS and U.S. officials) will be treated as indicated in paragraphs 5.4.a. and b., above.

d. (U) Exceptions: Notwithstanding the provisions of paragraphs 5.4.b. and c., the DIRNSA/CHCSS may waive the destruction requirement for international communicat ions containing, inter alia, the following types of information:

(1) Significant FOREIGN INTELLIGENCE, or

(2) Evidence of a crime or threat of death or serious bodily harm to any person, or

(3) Anomalies that reveal a potential vulnerability to U.S. communications security. Communications for which the Attorney General or DIRNSA/CHCSS's waiver is sought should be forwarded to NSA/CSS, Attn: Signals Intelligence Directorate Office of Oversight & Compliance (SV).

(U) Radio Communications

5.5. (U) Radio Communications with a Terminal in the UNITED STATES.

a. (~~S//SI//REL~~) All radio communications that pass over channels with a terminal in the UNITED STATES must be processed through a computer scan dictionary or similar device unless those communications occur over channels used exclusively by a FOREIGN POWER.

b. (~~S//SI//REL~~) International common-access radio communications that pass over channels with a terminal in the UNITED STATES, other than [redacted] comunications, may be processed without the use of a computer scan dictionary or similar device if necessary to determine whether a channel contains communications of FOREIGN INTELLIGENCE interest which NSA may wish to collect. Such processing may not exceed two hours without the specific prior written approval of the Signals Intelligence Director or a designee and, in any event, shall be limited to the minimum amount of time necessary to determine the nature of communications on the channel and the amount of such communications that include FOREIGN INTELLIGENCE. Once it is determined that the channel contains sufficient communications of FOREIGN INTELLIGENCE interest to warrant COLLECTION and exploitation to produce FOREIGN INTELLIGENCE, a computer scan dictionary or similar device must be used for additional processing.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

c. (U//~~FOUO~~) Copies of all written approvals made pursuant to 5.5.b. must be provided to the GC and the IG.

SECTION 6- (U) RETENTION

(U) Retention of Communications

6.1. (U) Retention of Communications to, from or About U.S. PERSONS.

a. (U) Except as otherwise provided in Annex A, Appendix 1, Section 4, communications to, from or about U.S. PERSONS that are intercepted by the USSS may be retained in their original or transcribed form only as follows:

(1) (U//FOUO) Unenciphered communications not thought to contain secret meaning may be retained for five years unless the Signals Intelligence Director determines in writing that retention for a longer period is required to respond to authorized FOREIGN INTELLIGENCE requirements.

(2) (U//FOUO) Communications necessary to maintain technical data bases for cryptanalytic or traffic analytic purposes may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future FOREIGN INTELLIGENCE requirement. Sufficient duration may vary with the nature of the exploitation and may consist of any period of time during which the technical data base is subject to, or of use in, cryptanalysis. If a U.S. PERSON'S identity is not necessary to maintaining technical data bases, it should be deleted or replaced by a generic term when practicable.

b. (U) Communications which could be disseminated under Section 7, below (i.e., without elimination of references to U.S. PERSONS) may be retained in their original or transcribed form.

(U) Access

6.2. (U) Access to raw traffic storage systems which contain identities of U.S. PERSONS must be limited to SIGINT production personnel or other persons who conduct signals intelligence activities under the direction, authority, or control of DIRNSA/CHCSS . For more information on access to SIGINT, refer to USSID CR1610, 2.3.

SECTION 7- (U) DISSEMINATION

(U) Focus of SIGINT Reports

7.1. (U) All SIGINT reports will be written so as to focus solely on the activities of foreign entities and persons and their agents. Except as provided in Section 7.2., FOREIGN INTELLIGENCE information concerning U.S. PERSONS must be disseminated in a manner which does not identify the U.S. PERSON. Generic or general terms or phrases must be substituted for the identity (e.g., "U.S. firm" for the specific name of a U.S. CORPORATION or "U.S. PERSON" for the specific name of a U.S. PERSON). Files containing the identities of U.S. persons deleted from SIGINT reports will be maintained for a maximum period of one year and any requests from SIGINT customers for such identities should be referred to the Signals Intelligence Directorate's Office of Information Sharing Services (S12).

(U) Dissemination of U.S. PERSON Identities

7.2. (U) SIGINT reports may include the identification of a U.S. PERSON only if one of the following conditions is met and a determination is made by the appropriate approval authority that the recipient has a need for the identity for the performance of his official duties:

a. (U) The U.S. PERSON has CONSENTED to the dissemination of communications of, or about, him or her and has executed the CONSENT form found in Annex H of this USSID, or

b. (U) The information is PUBLICLY AVAILABLE (i.e., the information is derived from unclassified information available to the general public), or

c. (U) The identity of the U.S. PERSON is necessary to understand the FOREIGN INTELLIGENCE information or assess its importance. The following nonexclusive list contains examples of the type of information that meet this standard:

(1) (U) FOREIGN POWER or AGENT OF A FOREIGN POWER. The information indicates that the U.S. PERSON is a FOREIGN POWER or an AGENT OF A FOREIGN POWER.

(2) (U) Unauthorized Disclosure of Classified Information. The

information indicates that the U.S. PERSON may be engaged in the unauthorized disclosure of classified information.

(3) (U) International Narcotics Activity. The information indicates that the individual may be engaged in international narcotics trafficking activities. (See Annex J of this USSID for further information concerning individuals involved in international narcotics trafficking).

(4) (U) Criminal Activity. The information is evidence that the individual may be involved in a crime that has been, is being, or is about to be committed, provided that the dissemination is for law enforcement purposes.

(5) (U) Intelligence TARGET. The information indicates that the U.S. PERSON may be the TARGET of hostile intelligence activities of a FOREIGN POWER.

(6) (U) Threat to Safety. The information indicates that the identity of the U.S. PERSON is pertinent to a possible threat to the safety of any person or organization, including those who are TARGETS, victims or hostages of INTERNATIONAL TERRORIST organizations. Reporting units shall identify to S12 any report containing the identity of a U.S. PERSON reported under this subsection (6). Field reporting to S12 should be in the form of a CRITICOMM message and include the report date-time-group (DTG), product serial number and the reason for inclusion of the U.S. PERSON'S identity.

(7) (U) Senior Executive Branch Officials. The identity is that of a senior official of the Executive Branch of the U.S. Government. In this case only the official's title will be disseminated. Domestic political or personal information on such individuals will be neither disseminated nor retained.

(U) Approval Authorities

7.3. (U) Approval authorities for the release of identities of U.S. persons under Section 7 are as follows:

a. (U) DIRNSA/CHCSS. DIRNSA/CHCSS must approve dissemination of:

(1) The identities of any senator, congressman, officer, or employee of the Legislative Branch of the U.S. Government.

(2) The identity of any person for law enforcement purposes.

b. (U) Field Units and NSA Headquarters Elements. All SIGINT production organizations are authorized to disseminate the identities of U.S. PERSONS when:

(1) The identity is pertinent to the safety of any person or organization;

(2) The identity is that of a senior official of the Executive Branch; or

(3) The U.S. PERSON has CONSENTED under paragraph 7.2.a. above.

c. (U) Signals Intelligence Director and Designees.

(1) In all other cases, U.S. PERSON identities may be released only with the prior approval of the Signals Intelligence Director, the Deputy Signals Intelligence Director, the Chief, S12, the Deputy Chief, S12, or the Senior Operations Officer of the National Security Operations Center.

(2) For law enforcement purposes involving narcotics related information, DIRNSA has granted to the Signals Intelligence Director authority to disseminate U.S. identities. This authority may not be further delegated.

(U) Privileged Communi-cations and Criminal Activity

7.4. (U) Privileged Communications and Criminal Activity. All proposed disseminations of information constituting U.S. PERSON privileged communications (e.g., attorney/client, doctor/patient) and all information concerning criminal activities or criminal or judicial proceedings in the UNITED STATES must be reviewed by the Office of General Counsel prior to dissemination.

(U) Improper Dissemination

7.5. (U) If the name of a U.S. PERSON is improperly disseminated, the incident should be reported to S12 and SV within 24 hours of discovery of the error.

SECTION 8 - (U) RESPONSIBILITIES

(U) Inspector General

8.1. (U) The Inspector General shall:

a. (U) Conduct regular inspections and perform general oversight of NSA/CSS activities to ensure compliance with this USSID.

b. (U) Establish procedures for reporting by NSA/CSS signals intelligence elements of their activities and practices for oversight purposes.

c. (U) Report to the DIRNSA/CHCSS, annually by 31 October, concerning NSA/CSS compliance with this USSID.

d. (U) Report quarterly with the DIRNSA/CHCSS and General Counsel to the President's Intelligence Oversight Board through the Assistant to the Secretary of Defense (Intelligence Oversight).

(U) General Counsel

8.2. (U) The General Counsel shall:

a. (U) Provide legal advice and assistance to all elements of the USSS regarding SIGINT activities. Requests for legal advice on any aspect of these procedures may be sent by CRITICOMM, secure email, or by NSA/CSS secure telephone 963-3121, STE [redacted] or non-secure (301) 688-5015. (b)(3)-P.L. 86-36

b. (U) Prepare and process all applications for Foreign Intelligence Surveillance Court orders and requests for Attorney General approvals required by these procedures.

c. (U) Advise the IG in inspections and oversight of USSS activities.

d. (U) Review and assess for legal implications as requested by the DIRNSA/CHCSS, Deputy Director, IG, Signals Intelligence Director, or their designees, all new major requirements and internally generated USSS activities.

e. (U) Advise USSS personnel of new legislation and case law that may affect USSS missions, functions, operations, activities, or practices.

f. (U) Report as required to the Attorney General and the President's Intelligence Oversight Board and provide copies of such reports to the DIRNSA/CHCSS and affected agency elements.

g. (U) Process requests from any DoD intelligence component for authority to use signals as described in Procedure 5, Part 5, of DoD 5240.1-R, for periods in excess of 90 days in the development, test, or calibration of ELECTRONIC SURVEILLANCE equipment and other equipment that can intercept communications.

(U) Signals Intelligence Director

8.3. (U) The Signals Intelligence Director shall:

a. (U) Ensure that all SIGINT production personnel understand and maintain a high degree of awareness and sensitivity to the requirements of this USSID.

b. (U) Apply the provisions of this USSID to all SIGINT production activities. The Signals Intelligence Directorate staff focal point for USSID SP0018 (formerly USSID 18) matters is SV.

c. (U) Conduct necessary reviews of SIGINT production activities and practices to ensure consistency with this USSID.

d. (U) Ensure that all new major requirements levied on the USSS or internally generated activities are considered for review by the GC. All activities that raise questions of law or the proper interpretation of this USSID must be reviewed by the GC prior to acceptance or execution.

(U) All Elements of the USSS

8.4. (U) All elements of the USSS shall:

a. (U) Implement this directive upon receipt.

b. (U) Prepare new procedures or amend or supplement existing procedures as required to ensure adherence to this USSID. A copy of such procedures shall be forwarded to NSA/CSS, Attn: SV.

c. (U) Immediately inform the Signals Intelligence Director of any tasking or instructions that appear to require actions at variance with this USSID.

d. (U) Promptly report to the NSA IG and consult with the NSA GC on all activities that may raise a question of compliance with this USSID.

SECTION 9 - (U) DEFINITIONS

(U) Agent of Foreign Power

9.1. (U) AGENT OF A FOREIGN POWER means:

a. (U) Any person, other than a U.S. PERSON, who:

(1) (U) Acts in the UNITED STATES as an officer or employee of a FOREIGN POWER, or as a member of a group engaged in INTERNATIONAL TERRORISM or activities in preparation therefore; or

(2) (U) Acts for, or on behalf of, a FOREIGN POWER that engages in clandestine intelligence activities in the UNITED STATES contrary to the interests of the UNITED STATES, when the circumstances of such person's presence in the UNITED STATES indicate that such person may engage in such activities in the UNITED STATES, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

b. (U) Any person, including a U.S. PERSON, who:

(1) (U) Knowingly engages in clandestine intelligence gathering activities for, or on behalf of, a FOREIGN POWER, which activities involve, or may involve, a violation of the criminal statutes of the UNITED STATES; or

(2) (U) Pursuant to the direction of an intelligence service or network of a FOREIGN POWER, knowingly engages in any other clandestine intelligence activities for, or on behalf of, such FOREIGN POWER, which activities involve or are about to involve, a violation of the criminal statutes of the UNITED STATES; or

(3) (U) Knowingly engages in sabotage or INTERNATIONAL TERRORISM, or activities that are in preparation thereof, for or on behalf of a FOREIGN POWER; or

(4) (U) Knowingly aids or abets any person in the conduct of activities described in paragraphs 9.1.b. (1) through (3) or knowingly conspires with any person to engage in those activities.

c. (U) For all purposes other than the conduct of ELECTRONIC SURVEILLANCE as defined by the Foreign Intelligence Surveillance Act (see Annex A), the phrase "AGENT OF A FOREIGN POWER" also means any person, including U.S. PERSONS outside the UNITED STATES, who are officers or employees of a FOREIGN POWER, or who act unlawfully for or pursuant to the direction of a FOREIGN POWER, or who are in contact with or acting in collaboration with an intelligence or security service of a FOREIGN POWER for the purpose of providing access to information or material classified by the UNITED STATES Government and to which the person has or has had access. The mere fact that a person's activities may benefit or further the aims of a FOREIGN POWER is not enough to bring that person under this provision, absent evidence that the person is taking direction from or acting in knowing concert with a FOREIGN POWER.

(U) Collection 9.2. (U) COLLECTION means intentional tasking or SELECTION of

identified nonpublic communications for subsequent processing aimed at reporting or retention as a file record.

(U) Communicant

9.3. (U) COMMUNICANT means a sender or intended recipient of a communication.

(U) Communications about a U.S. Person

9.4. (U) COMMUNICATIONS ABOUT A U.S. PERSON are those in which the U.S. PERSON is identified in the communication. A U.S. PERSON is identified when the person's name, unique title, address, or other personal identifier is revealed in the communication in the context of activities conducted by that person or activities conducted by others and related to that person. A mere reference to a product by brand name or manufacturer's name, e.g., "Boeing 707" is not an identification of a U.S. person.

(U) Consent

9.5. (U) CONSENT, for SIGINT purposes, means an agreement by a person or organization to permit the USSS to take particular actions that affect the person or organization. An agreement by an organization with the National Security Agency to permit COLLECTION of information shall be deemed valid CONSENT if given on behalf of such organization by an official or governing body determined by the GC, National Security Agency, to have actual or apparent authority to make such an agreement.

(U) Corporations

9.6. (U) CORPORATIONS, for purposes of this USSID, are entities legally recognized as separate from the persons who formed, own, or run them. CORPORATIONS have the nationality of the nation state under whose laws they were formed. Thus, CORPORATIONS incorporated under UNITED STATES federal or state law are U.S. PERSONS.

(U) Electronic Surveillance

9.7. (U) ELECTRONIC SURVEILLANCE means:

a. (U) In the case of an electronic communication, the acquisition of a nonpublic communication by electronic means without the CONSENT of a person who is a party to the communication.

b. (U) In the case of a nonelectronic communication, the acquisition of a nonpublic communication by electronic means without the CONSENT of a person who is visibly present at the place of communication.

c. (U) The term ELECTRONIC SURVEILLANCE does not include the use of radio direction finding equipment solely to determine the location of a transmitter.

(U) Foreign Communication

9.8. (U) FOREIGN COMMUNICATION means a communication that has at least one COMMUNICANT outside of the UNITED STATES, or that is entirely among FOREIGN POWERS or between a FOREIGN POWER and officials of a FOREIGN POWER, but does not include communications intercepted by ELECTRONIC SURVEILLANCE directed at premises in the UNITED STATES used predominantly for residential purposes.

(U) Foreign Intelligence

9.9. (U) FOREIGN INTELLIGENCE means information relating to the capabilities, intentions, and activities of FOREIGN POWERS, organizations, or persons, and for purposes of this USSID includes both positive FOREIGN INTELLIGENCE and counterintelligence.

(U) Foreign Power

9.10. (U) FOREIGN POWER means:

a. (U) A foreign government or any component thereof, whether or not recognized by the UNITED STATES,

b. (U) A faction of a foreign nation or nations, not substantially composed of UNITED STATES PERSONS,

c. (U) An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments,

d. (U) A group engaged in INTERNATIONAL TERRORISM or activities in preparation thereof,

e. (U) A foreign-based political organization, not substantially composed of UNITED STATES PERSONS, or

f. (U) An entity that is directed and controlled by a foreign government or governments.

(U) Interception

9.11. (U) INTERCEPTION means the acquisition by the USSS through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligible form, but does not include the display of signals on visual display devices intended to permit the examination of the technical characteristics of the signals without reference to the information content carried by the signal.

(U) International Terrorism

9.12. (U) INTERNATIONAL TERRORISM means activities that:

a. (U) Involve violent acts or acts dangerous to human life that are a

violation of the criminal laws of the UNITED STATES or of any State, or that would be a criminal violation if committed within the jurisdiction of the UNITED STATES or any State, and

b. (U) Appear to be intended:

(1) (U) to intimidate or coerce a civilian population,

(2) (U) to influence the policy of a government by intimidation or coercion, or

(3) (U) to affect the conduct of a government by assassination or kidnapping, and

c. (U) Occur totally outside the UNITED STATES, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

(U) Publicly Available Information

9.13. (U) PUBLICLY AVAILABLE INFORMATION means information that has been published or broadcast for general public consumption, is available on request to a member of the general public, has been seen or heard by a casual observer, or is made available at a meeting open to the general public.

(U) Selection

9.14. ~~(S//SI//REL)~~ SELECTION, as applied to manual and electronic processing activities, means the intentional insertion of a [redacted] telephone number, email address, [redacted] into a computer scan dictionary or manual scan guide for the purpose of identifying messages of interest and isolating them for further processing.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

(U) Selection Term

9.15. (U//~~FOUO~~) SELECTION TERM means the composite of individual terms used to effect or defeat SELECTION of particular communications for the purpose of INTERCEPTION. It comprises the entire term or series of terms so used, but not any segregable term contained therein. It applies to both electronic and manual processing.

(U) Target

9.16. (U) TARGET, OR TARGETING: See COLLECTION.

(U) United States

9.17. (U) UNITED STATES, when used geographically, includes the 50 states and the District of Columbia, Puerto Rico, Guam, American Samoa, the U.S. Virgin Islands, the Northern Mariana Islands, and any other territory or

possession over which the UNITED STATES exercises sovereignty.

(U) United States Person

9.18. (U) UNITED STATES PERSON:

a. (U) A citizen of the UNITED STATES,

b. (U) An alien lawfully admitted for permanent residence in the UNITED STATES,

c. (U) Unincorporated groups and associations a substantial number of the members of which constitute a. or b. above, or

d. (U) CORPORATIONS incorporated in the UNITED STATES, including U.S. flag nongovernmental aircraft or vessels, but not including those entities which are openly acknowledged by a foreign government or governments to be directed and controlled by them.

e. (U) The following guidelines apply in determining whether a person is a U.S. PERSON:

(1) (U) A person known to be currently in the United States will be treated as a U.S. PERSON unless that person is reasonably identified as an alien who has not been admitted for permanent residence or if the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is not a U.S. PERSON.

(2) (U) A person known to be currently outside the UNITED STATES, or whose location is not known, will not be treated as a U.S. PERSON unless such person is reasonably identified as such or the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is a U.S. PERSON.

(3) (U) A person known to be an alien admitted for permanent residence may be assumed to have lost status as a U.S. PERSON if the person leaves the UNITED STATES and it is known that the person is not in compliance with the administrative formalities provided by law (8 U.S.C. Section 1203) that enable such persons to reenter the UNITED STATES without regard to the provisions of law that would otherwise restrict an alien's entry into the UNITED STATES. The failure to follow the statutory procedures provides a reasonable basis to conclude that such alien has abandoned any intention of maintaining status as a permanent resident alien.

(4) (U) An unincorporated association whose headquarters are located outside the UNITED STATES may be presumed not to be a U.S. PERSON unless the USSS has information indicating that a substantial number of members are citizens of the UNITED STATES or aliens lawfully admitted for permanent residence.

(5) (U) CORPORATIONS have the nationality of the nation/state in which they are incorporated. CORPORATIONS formed under U.S. federal or state law are thus U.S. persons, even if the corporate stock is foreign-owned. The only exception set forth above is CORPORATIONS which are openly acknowledged to be directed and controlled by foreign governments. Conversely, CORPORATIONS incorporated in foreign countries are not U.S. PERSONS even if that CORPORATION is a subsidiary of a U.S. CORPORATION.

(6) (U) Nongovernmental ships and aircraft are legal entities and have the nationality of the country in which they are registered. Ships and aircraft fly the flag and are subject to the law of their place of registration.

USSID SP0018

ANNEX A - (U) PROCEDURES IMPLEMENTING TITLE I OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

SECTION 1 - (U) PURPOSE AND APPLICABILITY

(U) Foreign Intelligence Surveillance Act

A1.1. (U) Title I of the Foreign Intelligence Surveillance Act (the Act) governs the conduct of certain electronic surveillance activities within the United States to collect foreign intelligence information.

A1.2. (U) Title I of the Act covers the intentional collection of the communications of a particular, known U.S. person who is in the United States,

all wiretaps in the United States, the acquisition of certain radio communications where all parties to that communication are located in the United States, and the monitoring of information in which there is a reasonable expectation of privacy.

A1.3. (U) The Act requires that all such surveillances be directed only at foreign powers and their agents as defined by the Act and that all such surveillances be authorized by the United States Foreign Intelligence Surveillance Court, or in certain limited circumstances, by the Attorney General.

SECTION 2 - (U) GENERAL

(U) PROCEDURE AND STANDARDS

A2.1. (U) Procedures and standards for securing Court orders or Attorney General certifications to conduct electronic surveillances are set forth in the Act. Requests for such orders or certifications should be forwarded by the appropriate Key Component through the NSA GC to the DIRNSA/CHCSS and should be accompanied by a statement of the facts and circumstances justifying a belief that the target is a foreign power or an agent of a foreign power and that each of the facilities or places at which the surveillance will be directed are being used, or are about to be used, by that foreign power or agent.

A2.2. (U) If the proposed surveillance meets the requirements of the Act and the Director approves the proposal, attorneys in the OGC will draw the necessary court application or request for Attorney General certification.

SECTION 3 - (U) MINIMIZATION PROCEDURES

(U) Surveillances

A3.1. (U//~~FOUO~~) Surveillances authorized by the Act are required to be carried out in accordance with the Act and pursuant to the court order or Attorney General certification authorizing that particular surveillance. In some cases, the court orders are tailored to address particular problems, and in those instances the NSA attorney will advise the appropriate NSA offices of the terms of the court's orders. In most cases, however, the court order will incorporate without any changes the standardized minimization procedures set forth in Appendix I.

SECTION 4 - (U) RESPONSIBILITIES

(U) General Counsel Responsibilities

A4.1. (U) The GC will review all requests to conduct electronic surveillances as defined by the Act, prepare all applications and materials required by the Act, and provide pertinent legal advice and assistance to all elements of the United

States SIGINT System.

(U) Inspector General Responsiblities

A4.2. (U) The IG will conduct regular inspections and oversight of all SIGINT activities to assure compliance with this Directive.

(U) SIGINT Manager and Supervisor Responsiblities

A4.3. (U) All SIGINT managers and supervisors with responsibilities relating to the Act will ensure that they and their personnel are thoroughly familiar with the Act, its implementing procedures, and any court orders or Attorney General certifications pertinent to their mission. Personnel with duties related to the Act will consult the GC's office for any required legal advice and assistance or training of newly assigned personnel.

A4.4. (U) Appropriate records will be maintained demonstrating compliance with the terms of all court orders and Attorney General certifications, and any discrepancies in that regard will be promptly reported to the offices of the GC and IG.

USSID SP0018, ANNEX A

APPENDIX 1 - (U) STANDARD MINIMIZATION PROCEDURES FOR ELECTRONIC SURVEILLANCE CONDUCTED BY THE NATIONAL SECURITY AGENCY (NSA)

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

STANDARD MINIMIZATION

PROCEDURES FOR ELECTRONIC SURVEILLANCE

CONDUCTED BY THE NATIONAL SECURITY AGENCY (NSA)

Pursuant to Section 101(h) of the Foreign Intelligence Surveillance Act of 1978 (hereinafter "the Act"), the following procedures have been adopted by the Attorney General and shall be followed by the NSA in implementing this electronic surveillance: (U)

SECTION 1 - APPLICABILITY AND SCOPE (U)

These procedures apply to the acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that is collected in the course of electronic surveillance as ordered by the United States Foreign Intelligence Surveillance Court under Section 102(b) or authorized by Attorney General Certification under Section 102(a) of the Act. These procedures also apply to non-United States persons where specifically indicated. (U)

SECTION 2 - DEFINITIONS (U)

In addition to the definitions in Section 101 of the Act, the following definitions shall apply to these procedures:

(a) Acquisition means the collection by NSA through electronic means of a nonpublic communication to which it is not an intended party. (U)

(b) Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly available information about the person. (U)

(c) Communications of a United States person include all communications to which a United States person is a party. (U)

(d) Consent is the agreement by a person or organization to permit the NSA to take particular actions that affect the person or organization. To be effective, consent must be given by the affected person or organization with sufficient knowledge to understand the action that may be taken and the possible consequences of that action. Consent by an organization shall be deemed valid if given on behalf of the organization by an official or governing body determined by the General Counsel, NSA, to have actual or apparent authority to make such an agreement. (U)

(e) Foreign communication means a communication that has at least one communicant outside of the United States, or that is entirely among:

(1) foreign powers;

(2) officers and employees of foreign powers; or

(3) a foreign power and officers or employees of a foreign power.

All other communications are domestic communications. ~~(S-CCO)~~

(f) Identification of a United States person means the name, unique title, address, or other personal identifier of a United States person in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not an identification of a United States person. ~~(S-CCO)~~

(g) Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection. (U)

(h) <u>Publicly available information</u> means information that a member of the public could obtain on request, by research in public sources, or by casual observation. (U)

(i) <u>Technical data base</u> means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes. ~~(S-CCO)~~

(j) <u>United States person</u> means a United States person as defined in the Act. The following guidelines apply in determining whether a person whose status is unknown is a United States person: (U)

(1) A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence, or unless the nature or circumstances of the person's communications give rise to a reasonable belief that such person is not a United States person. (U)

(2) A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person. (U)

(3) A person known to be an alien admitted for permanent residence loses status as a United States person if the person leaves the United States and is not in compliance with Title 8, United States Code, Section 1203 enabling re-entry into the United States. Failure to follow the statutory procedures provides a reasonable basis to conclude that the alien has abandoned any intention of maintaining his status as a permanent resident alien. (U)

(4) An unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a United States person unless there is information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence. (U)

<u>SECTION 3 - ACQUISITION AND PROCESSING – GENERAL (U)</u>

(a) <u>Acquisition (U)</u>

The acquisition of information by electronic surveillance shall be made in accordance with the certification of the Attorney General or the court order authorizing such surveillance and conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the surveillance. ~~(S-CCO)~~

(b) <u>Verification (U)</u>

At the initiation of the electronic surveillance, the NSA or the Federal Bureau of Investigation, if providing operational support, shall verify that the communication lines or telephone numbers being targeted are the lines or numbers of the target authorized by court order or Attorney General certification. Thereafter, collection personnel will monitor the acquisition of raw data at regular intervals to verify that the surveillance is not avoidably acquiring communications outside the authorized scope of the surveillance or information concerning United States persons not related to the purpose of the surveillance. ~~(S-CCO)~~

(c) <u>Monitoring, Recording, and Processing (U)</u>

(1) Electronic surveillance of the target may be monitored contemporaneously, recorded automatically, or both. (U)

(2) Personnel who monitor the electronic surveillance shall exercise reasonable judgement in determining whether particular information acquired must be minimized and shall destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle at which such communication can be identified either as clearly not relevant to the authorized purpose of the surveillance (i.e., the communication does not contain foreign intelligence information) or as containing evidence of a crime which may be disseminated under these procedures. ~~(S-CCO)~~

(3) Communications of or concerning United States persons that may be related to the authorized purpose of the surveillance may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such communications or information may be retained and disseminated only in accordance with Sections 4, 5, and 6 of these procedures. ~~(C)~~

(4) Magnetic tapes or other storage media that contain acquired communications may be processed. ~~(S-CCO)~~

(5) Each communication shall be reviewed to determine whether it is a domestic or foreign communication to or from the targeted premises and is reasonably believed to contain foreign intelligence information or evidence of a crime. Only such communications may be processed. All other communications may be retained or disseminated only in accordance with Sections 5 and 6 of these procedures. ~~(S-CCO)~~

(6) Magnetic tapes or other storage media containing foreign communications may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, shall not include United States person names or identifiers and shall be limited to those selection terms reasonably likely to identify [redacted] that are authorized for intentional collection under Executive Order 12333 implementing procedures. ~~(S-CCO)~~

(b)(1)

(7) Further processing, retention and dissemination of foreign communications shall be made in accordance with Sections 4, 6, and 7, as applicable, below. Further processing, storage and dissemination of inadvertently acquired domestic communications shall be made in accordance with Sections 4 and 5 below. ~~(S-CCO)~~

(d) <u>U.S. Persons Employed by the Foreign Power</u> ~~(C)~~

Communications of or concerning United States persons employed by a foreign power may be used and retained as otherwise provided in these procedures except that:

(1) Such United States persons shall not be identified in connection with any communication that the person places or receives on behalf of another unless the identification is permitted under Section 6 of these procedures; and

(2) personal communications of United States persons that could not be foreign intelligence may only be retained, used, or disseminated in accordance with Section 5 of these procedures. ~~(S-CCO)~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

(e) <u>Destruction of Raw Data</u> ~~(C)~~

Communications and other information, including that reduced to graphic or "hard copy" form such as [redacted] shall be reviewed for retention in accordance with the standards set forth in these procedures. Communications and other information, in any form, that do not meet

such retention standards and that are known to contain communications of or concerning United States persons shall be promptly destroyed. ~~(S-CCO)~~

(f) Non-pertinent Communications (U)

(1) Communications determined to fall within established categories of non-pertinent communications, such as those set forth in subparagraph (6) of this section, should not be retained unless they contain information that may be disseminated under Sections 5, 6, or 7 below. (U)

(2) Monitors may listen to all communications, including those that initially appear to fall within established categories until they can reasonably determine that the communication cannot be disseminated under Sections 5, 6, or 7 below. ~~(S-CCO)~~

(3) Communications of United States persons will be analyzed to establish categories of communications that are not pertinent to the authorized purpose of the surveillance. (U)

(4) These categories should be established after a reasonable period of monitoring the communications of the targets. (U)

(5) Information that appears to be foreign intelligence may be retained even if it is acquired as a part of a communication falling within a category that is generally non-pertinent. ~~(S-CCO)~~

(6) Categories of non-pertinent communications which may be applied in these surveillance include:

(A) Calls to and from United States Government officials;

(B) Calls to and from children;

(C) Calls to and from students for information to aid them in academic endeavors;

(D) Calls between family members; and

(E) Calls relating solely to personal services, such as food orders, transportation, etc. ~~(S-CCO)~~

(g) Change in Target's Location or Status ~~(S-CCO)~~

(1) During periods of known extended absence by a targeted agent of a foreign power from premises under surveillance, only communications to which the target is a party may be retained and disseminated. ~~(S-CCO)~~

(2) When there is reason to believe that the target of an electronic surveillance is no longer a foreign power or an agent of a foreign power, or no longer occupies the premises authorized for surveillance, that electronic surveillance shall be immediately terminated, and shall not resume unless subsequently approved under the Act. When any person involved in collection or processing of an electronic surveillance being conducted pursuant to the Act becomes aware of information tending to indicate a material change in the status or location of a target, the person shall immediately ensure that the NSA's Office of General Counsel is also made aware of such information. ~~(S-CCO)~~

SECTION 4 - ACQUISITION AND PROCESSING - SPECIAL PROCEDURES (U)

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

(a) Collection Against Residential Premises ~~(S-CCO)~~

(b)(1)

(1) An electronic surveillance directed against premises located in the United States and used for residential purposes shall be conducted by technical means designed to limit the information acquired to communications that have one communicant outside the United States, [redacted] The technical means employed shall consist of [redacted] equipment or equipment capable of identifying international [redacted] or other particular international communications known to be used by the targeted foreign power and its agents. Communications to or from the target residential premises that are processed [redacted] of a foreign power or agent of a foreign power located in a foreign country, or on the foreign country or foreign city telephone direct dialing codes (area codes) for the areas in which such foreign powers or agents are located. ~~(S-CCO)~~

(2) [redacted] ~~(S-CCO)~~

(3) Domestic communications that are incidentally acquired during collection against residential premises shall be handled under Section 5 of these procedures. ~~(S-CCO)~~

(b) Attorney-Client Communications ~~(C)~~

As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment and an attorney who represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring of that communication will cease and the communication shall be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the tape containing that conversation will be placed under seal and the Department of Justice, Office of Intelligence Policy and Review, shall be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein. ~~(S-CCO)~~

SECTION 5 - DOMESTIC COMMUNICATIONS (U)

(a) Dissemination (U)

Communications identified as domestic communications shall be promptly destroyed, except that:

(1) domestic communications that are reasonably believed to contain foreign intelligence information shall be disseminated to the Federal Bureau of Investigation (including United States person identities) for possible further dissemination by the Federal Bureau of Investigation in accordance with its minimization procedures;

(2) domestic communications that do not contain foreign intelligence information, but that are reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed, shall be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with Section 106(b) of the Act and crimes reporting procedures approved by the Secretary of Defense and the Attorney General; and

(3) domestic communications that are reasonably believed to contain technical data base information, as defined in Section 2(i), may be disseminated to the Federal Bureau of Investigation and to other elements of the U.S. SIGINT system. (S-CCO)

(b) Retention (U)

(1) Domestic communications disseminated to Federal law enforcement agencies may be retained by the NSA for a reasonable period of time, not to exceed six months (or any shorter period set by court order), to permit law enforcement agencies to determine whether access to original recordings of such communications is required for law enforcement purposes. (S-CCO)

(2) Domestic communications reasonably believed to contain technical data base information may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation. (S-CCO)

a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis. (S-CCO)

b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is one year unless the Deputy Director for Operations, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements. (S-CCO)

SECTION 6 - FOREIGN COMMUNICATIONS OF OR CONCERNING UNITED STATES PERSONS (U)

(a) Retention (U)

Foreign communications of or concerning United States persons acquired by the NSA in the course of an electronic surveillance subject to these procedures may be retained only:

(1) if necessary for the maintenance of technical data bases. Retention for this purpose is permitted for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.

a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is one year unless the Deputy Director for Operations, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements;

(2) if dissemination of such communications with reference to such United States persons would be permitted under subsection (b) below; or

(3) if the information is evidence of a crime that has been, is being, or is about to be committed and is provided to appropriate federal law enforcement authorities. (~~S-CCO~~)

(b) Dissemination (U)

A report based on communications of or concerning a United States person may be disseminated in accordance with Section 7 if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person. Otherwise dissemination of intelligence reports based on communications of or concerning a United States person may only be made to a recipient requiring the identity of such person for the performance of official duties but only if at least one of the following criteria is also met:

(1) the United States person has consented to dissemination or the information of or concerning the United States person is available publicly;

(2) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch;

(3) the communication or information indicates that the United States person may be:

(A) an agent of a foreign power;

(B) a foreign power as defined in Section 101(a)(4) or (6) of the Act;

(C) residing outside the United States and holding an official position in the government or military forces of a foreign power

(D) a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

(E) acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material.

(4) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;

(5) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information, but only after the agency that originated the information certifies that it is properly classified;

(6) the communication or information indicates that the United States person may be engaging in international terrorist activities;

(7) the acquisition of the United States person's communication was authorized by a court order issued pursuant to Section 105 of the Act and the communication may relate to the foreign intelligence purpose of the surveillance;

(8) the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes and is made in

accordance with Section 106(b) of the Act and crimes reporting procedures approved by the Secretary of Defense and the Attorney General. (U)

SECTION 7 - OTHER FOREIGN COMMUNICATIONS (U)

Foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy. (U)

SECTION 8 - COLLABORATION WITH FOREIGN GOVERNMENTS ~~(S-CCO)~~

(a) The sharing or exchange of foreign communications governed by these procedures with signals intelligence authorities of collaborating foreign governments (Second Parties) may be undertaken by the NSA only with the written assurance of the Second Party that the use of those foreign communications will be subject to the retention and dissemination provisions of these procedures. ~~(S-CCO)~~

(b) Domestic communications and communications to or from United States persons shall not be shared with Second Parties. ~~(S-CCO)~~

(c) Foreign plain text communications may be shared with Second Parties if they are first reviewed by NSA analysts, who shall remove references to United States persons that are not necessary to understand or assess the foreign intelligence information contained therein. ~~(S-CCO)~~

(d) Foreign enciphered or encoded communications may be shared with Second Parties without such prior review, provided that at least annually a representative sampling of those shared communications that can be deciphered or decoded is reviewed by the NSA to ensure that any references therein to United States persons are necessary to understand or assess the foreign intelligence information being disseminated. Corrective measures with respect to each target or line shall be undertaken as necessary to maintain compliance with the above dissemination standard. The results of each review shall be made available to the Attorney General or a designee. ~~(S-CCO)~~

Approved by Attorney General Janet Reno on 1 July 1997

USSID SP0018

ANNEX B - (U) OPERATIONAL ASSISTANCE TO THE FEDERAL BUREAU OF INVESTIGATION

SECTION 1 - (U) GENERAL

(U) Operational Assistance

B1.1. (U) In accordance with the provisions of Section 2.6 of E.O. 12333, and the NSA/FBI Memorandum of Understanding of 25 November 1980, the National Security Agency may provide specialized equipment and technical knowledge to the FBI to assist the FBI in the conduct of its lawful functions. When requesting such assistance, the FBI will certify to the General Counsel of NSA/CSS that such equipment or technical knowledge is necessary to the accomplishment of one or more of the FBI's lawful functions.

B1.2. (U) NSA/CSS may also provide expert personnel to assist FBI personnel in the operation or installation of specialized equipment when that equipment is to be employed to collect foreign intelligence. When requesting the assistance of expert personnel, the FBI will certify to the General Counsel that such assistance is necessary to collect foreign intelligence and that the approval of the Attorney General (and, when necessary, a warrant from a court of competent jurisdiction) has been obtained.

SECTION 2 - (U) CONTROL

(U) Operational Control

B2.1. (U) No operational assistance as discussed in Section 1 shall be provided without the express permission of the DIRNSA/CHCSS, Deputy Director, NSA/CSS, the SIGINT Director, or the Deputy Director for Technology and Systems. The SIGINT Director and the Director of the Technology Directorate may approve requests for such assistance only with the concurrence of the General Counsel.

USSID SP0018

ANNEX C - (U) SIGNALS INTELLIGENCE SUPPORT TO U.S. AND ALLIED MILITARY EXERCISE COMMAND AUTHORITIES

SECTION 1 - (U) POLICY

(U) SIGINT Support

C1.1. (U//FOUO) Signals Intelligence support to U.S. and Allied military exercise command authorities is provided for in USSID CR1221 and DoD Directive 5200.17 (M-2). Joint Chiefs of Staff Memorandum MJCS111-88, 18 August 1988, and USSID CR1200, 16 December 1988, establish doctrine and procedures for providing signals intelligence support to military commanders. The procedures in this Annex provide policy guidelines for safeguarding the rights of U.S. persons in the conduct of exercise SIGINT support activities.

SECTION 2 - (U) DEFINITIONS

(U) Military Tactical Communi-cations

C2.1. (U) United States and Allied military exercise communications, within the United States and abroad, that are necessary for the production of simulated foreign intelligence and counterintelligence or to permit an analysis of communications security.

SECTION 3 - (U) PROCEDURES

(U) Handling of Military Tactical Communi-cations

C3.1. (U//FOUO) The USSS may collect, process, store, and disseminate military tactical communications that are also communications of, or concerning, U.S. persons.

a. (U//FOUO) Collection efforts will be conducted in such a manner as to avoid, to the extent feasible, the intercept of non-exercise-related communications.

b. (U//FOUO) Military tactical communications may be stored and processed without deletion of references to U.S. persons if the names and communications of the U.S. persons who are exercise participants, whether military, government, or contractor, are contained in, or such communications constitute, exercise-related communications or fictitious communications or information prepared for the exercise.

c. (U//FOUO) Communications of U.S. persons not participating in the exercise that are inadvertently intercepted during the exercise shall be destroyed as soon as feasible, provided that a record describing the signal or frequency user in technical and generic terms may be retained for signal identification and Collection-avoidance purposes.

Inadvertently intercepted communications that contain anomalies in enciphered communicatioins that reveal a potential vulnerability to United States communications security should be forwarded to the Information Assurance Director.

d. (U//~~FOUO~~) Dissemination of military exercise communications, exercise reports, or information files derived from such communications shall be limited to those authorities and persons participating in the exercise or conducting reviews and critiques thereof.

USSID SP0018

ANNEX D - (U) TESTING OF ELECTRONIC EQUIPMENT

SECTION 1 - (U) PURPOSE AND APPLICABILITY

(U) Testing of Electronic Equipment

D1.1. (U) This Annex applies to the testing of electronic equipment that has the capability to intercept communications and other non-public information. Testing includes development, calibration, and evaluation of such equipment, and will be conducted, to the maximum extent practical, without interception or monitoring of U.S. persons.

SECTION 2 - (U) PROCEDURES

(U) Testing Limitations

D2.1. (U) The USSS may test electronic equipment that has the capability to intercept communications and other information subject to the following limitations:

a. (U) To the maximum extent practical, the following should be used:

(1) (U) Laboratory-generated signals;

(2) (U) Communications transmitted between terminals located outside the United States not used by any known U.S. person;

(3) (U) Official government agency communications with the consent of an appropriate official of that agency, or an individual's communications with the consent of that individual;

(4) (U) Public broadcast signals; or

(5) (U) Other communications in which there is no reasonable expectation of privacy (as approved in each instance by the NSA/CSS General Counsel).

b. (U) Where it is not practical to test electronic equipment solely against signals described in paragraph D2.1.a., above, testing may be conducted, provided:

(1) (U) The proposed test is coordinated with the NSA/CSS General Counsel;

(2) (U) The test is limited in scope and duration to that necessary to determine the capability of the equipment;

(3) (U) No particular person is targeted without consent and it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance; and

(4) (U) The test does not exceed 90 calendar days.

c. (U) Where the test involves communications other than those identified in paragraph D2.1.a. and a test period longer than 90 days is required, the Foreign Intelligence Surveillance Act requires that the test be approved by the Attorney General. Such proposals and plans shall be submitted by USSS elements through the General Counsel, NSA/CSS, to the DIRNSA/CHCSS for transmission to the Attorney General. The test proposal shall state the requirement for an extended test involving such communications, the nature of the test, the organization that will conduct the test, and the proposed disposition of any signals or communications acquired during the test.

D2.2. (U) The content of any communication other than communications between non-U.S. persons outside the United States which are acquired during a test and evaluation shall be:

a. (U) Retained and used only for the purpose of determining the capability of the electronic equipment;

b. (U) Disclosed only to persons conducting or evaluating the test; and

c. (U) Destroyed before or immediately upon completion of the testing.

D2.3. (U) The technical parameters of a communication, such as frequency, modulation, and time of activity of acquired electronic signals, may be retained and used for test reporting or collection-avoidance purposes. Such parameters may be disseminated to other DoD intelligence components and other entities authorized to conduct electronic surveillance, provided such dissemination and use are limited to testing, evaluation, or collection-avoidance purposes.

ANNEX E - (U) SEARCH AND DEVELOPMENT OPERATIONS

SECTION 1 - (U) PROCEDURES

(U) Procedures for Safeguarding the Rights of U.S. Persons

E1.1. (U) This Annex provides the procedures for safeguarding the rights of U.S. persons when conducting SIGINT search and development activities.

E1.2. (U//~~FOUO~~) The USSS may conduct search and development activities with respect to signals throughout the radio spectrum under the following limitations:

a. (U) Signals may be collected only for the purpose of identifying those signals that:

(1) (U) May contain information related to the production of foreign intelligence or counterintelligence;

(2) U) Are enciphered or appear to contain secret meaning;

(3) (U) Are necessary to assure efficient signals intelligence collection or to avoid the collection of unwanted signals; or

(4) ~~(S//SI//REL)~~ Reveal vulnerabilities of United States communications security.

b. ~~(S//SI//REL)~~ Communications originated or intended for receipt in the United States or originated or intended for receipt by U.S. persons shall be processed in accordance with Section 5 of USSID SP0018, provided that information necessary for cataloging the constituent elements of the signal environment may be processed and retained if such information does not identify a U.S. person. Information revealing a United States communications security vulnerability may be retained.

c. ~~(S//SI//REL)~~ Information necessary for cataloging the constituent elements of the signal environment may be disseminated to the extent such information does not identify U.S. persons. Communications equipment nomenclature may be disseminated. Information that reveals a vulnerability to United States communications security may be disseminated to the appropriate communications security authorities.

d. (U) All information obtained in the process of search and development that appears to be of foreign intelligence value may be forwarded to the proper analytic office within NSA/CSS for processing and dissemination in accordance with relevant portions of this USSID.

USSID SP0018

ANNEX F - (U) ILLICIT COMMUNICATIONS

SECTION 1 - (U) PROCEDURES

(U) Handling of Illicit Communications

F1.1. (U) The USSS may collect, retain, process, and disseminate illicit communications without reference to the requirements concerning U.S. persons.

F1.2. (U//FOUO) The term "illicit communications" means a communication transmitted in violation of either the Communications Act of 1934 and regulations issued thereunder or international agreements, which because of its explicit content, message characteristics, or method of transmission, is reasonably believed to be a communication to or from an agent or agents of foreign powers, whether or not U.S. persons.

USSID SP0018

ANNEX G - (U) TRAINING OF PERSONNEL IN THE OPERATION AND USE OF SIGINT COLLECTION AND OTHER SURVEILLANCE EQUIPMENT

SECTION 1 - (U) APPLICABILITY

(U) Purpose

G1.1. (U) This Annex applies to all USSS use of SIGINT collection and other surveillance equipment for training purposes.

SECTION 2 - (U) POLICY

(U) Training

G2.1. (U) Training of USSS personnel in the operation and use of SIGINT collection equipment shall be conducted, to the maximum extent that is practical, without interception of the communications of U.S. persons or persons in the United States who have not given consent to such interception. Communications and information protected by

the Foreign Intelligence Surveillance Act (FISA) (see Annex A) will not be collected for training purposes.

SECTION 3 - (U) PROCEDURES

(U) Training Guidance

G3.1. (U) The training of USSS personnel in the operation and use of SIGINT collection and other surveillance equipment shall include guidance concerning the requirements and restrictions of the FISA , Executive Order 12333, and this USSID.

G3.2. (U) The use of SIGINT collection and other surveillance equipment for training purposes is subject to the following limitations:

a. (U) To the maximum extent practical, use of such equipment for training purposes shall be directed against otherwise authorized intelligence targets;

b. (U) The contents of private communications of nonconsenting U.S. persons may not be acquired unless the person is an authorized target of electronic surveillance; and

c. (U) The electronic surveillance will be limited in extent and duration to that necessary to train personnel in the use of the equipment.

G3.3. (U) The limitations in paragraph G3.2. do not apply in the following instances:

a. (U) Public broadcasts, distress signals, or official United States Government communications may be monitored, provided that, where government agency communications are monitored, the consent of an appropriate official is obtained; and

b. (U) Minimal acquisition of information is permitted as required for calibration purposes.

G3.4. (U) Information collected during training that involves authorized intelligence targets may be retained in accordance with Section 6 of this USSID and disseminated in accordance with Section 7 of this USSID. Information other than distress signals collected during training that does not involve authorized intelligence targets or that is acquired inadvertently shall be destroyed as soon as practical or upon completion of the training and may not be disseminated outside the USSS for any purpose. Distress signals should be referred to the SIGINT Director.

USSID SP0018

ANNEX H - (U) CONSENT FORMS

SECTION 1 - (U) PURPOSE

(U) Forms

H1.1. (U) The forms set forth in this Annex have been approved by the National Security Agency's Office of General Counsel (NSA OGC) to obtain and record the express consent of a U.S. person for elements of the United States SIGINT System (USSS) to collect and disseminate communications of or concerning that person for foreign intelligence purposes, to include but not limited to force protection, hostage recovery, and other like purposes.

H1.2. (U//FOUO) Forms 1 and 2 can be used to obtain and record consent to collect and disseminate a U.S. person's communications as well as references to the U.S. person in communications. Forms 3 and 4 only provide consent to collect and disseminate references to the U.S. person but neither Form 3 nor Form 4 provides consent to collect communications to or from the U.S. person who has executed the form. Each form contained in this Annex may be reproduced, provided the security classifications (top and bottom) are removed. It is the responsibility of the user to properly reclassify the consent form that is suitable to the user's purposes in accordance with requisite security guidelines and operational considerations of the customer whom the USSS is supporting.

H1.3. (U) Section 4.1.c. of United States Signals Intelligence Directive SP0018 states that the Director of NSA (DIRNSA) has authority to approve the consensual collection of communications to, from, or about U.S. persons. Elements of the USSS proposing to conduct consensual collection should forward a copy of the executed consent form and any pertinent information to the DIRNSA (or to the Senior Operations Officer of the National Security Operations Center) for approval of the proposed consensual collection activity. NSA OGC must also be notified promptly of the proposed collection activity.

H1.4. (U) If operational circumstances dictate, consent may be obtained orally or may be recorded on a form other than one of the forms contained in this Annex. However, any other form or method that is used to obtain and record a U.S. person's consent for elements of the USSS to collect and disseminate communications of or concerning that person must be reviewed and approved by NSA OGC.

CONSENT FORM 1

NSA SIGNALS INTELLIGENCE CONSENT AGREEMENT

I, _____________________________ _______, hereby consent to the National Security Agency or other elements of the United States Signals Intelligence System undertaking to seek and disseminate communications to, from, or referencing me for the purpose of:

_________________________________ _________________________________ ______________

_________________________________ _________________________________ ______________

I understand that, unless specified otherwise in the purpose above, communications to, from, or referencing me may be sought and disseminated while I am in the U.S. during the effective period of my consent. This consent applies to administrative messages alerting elements of the United States Signals Intelligence System to this consent, as well as to any signals intelligence reports that may relate to the purpose stated above.

Except as otherwise provided by law, to include procedures under Executive Order 12333, this consent covers only information that relates to the purpose stated above and is effective for the period:

_________________________________ _ to _________________________________ _

Signals intelligence reports containing information derived from communications to, from, or referencing me may only be disseminated to me and to _____________________________ ___________________, and to others as specified by the U.S. Government as otherwise permitted by law, to include procedures under Executive Order 12333.

_________________________________ ___ ______________ __

Signature Date

_________________________________ ___

Title

PRIVACY ACT STATEMENT: Authority for collecting information is contained in Section 6 of the National Security Agency Act of 1959, Public Law 86-36, codified at 50 U.S.C. 402 note; Executive Order (E.O.) 12333, as amended; and E.O. 13526. NSA's Blanket Routine Uses found at 58 Fed. Reg. 10,531 (1993) and the specific uses found in GNSA 18 apply to this information. Disclosure of requested information is voluntary but refusal to provide requested information may prevent NSA from effecting this consent form.

CONSENT FORM 2

CONSENT AGREEMENT

I, ____________________________ _______, hereby consent to the U.S. Government undertaking to seek and disseminate communications to, from, or referencing me for the purpose of:

________________________________ ________________________________ ______________

________________________________ ________________________________ ______________

I understand that, unless specified otherwise in the purpose above, communications to, from, or referencing me may be sought and disseminated while I am in the U.S. during the effective period of my consent. This consent applies to administrative messages alerting elements of the U.S. Government to this consent, as well as to any reports that may relate to the purpose stated above.

Except as otherwise provided by law, to include applicable U.S. Government procedures, this consent covers only information that relates to the purpose stated above and is effective for the period:

________________________________ _ to ________________________________ _.

Reports containing information derived from communications to, from, or referencing me may only be disseminated to me and to ____________________________ ___________________, and to others as specified by the U.S. government as otherwise permitted by law, to include applicable U.S. Government procedures.

________________________________ ___ _______________

Signature Date

________________________________ ___

Title

PRIVACY ACT STATEMENT: Authority for collecting information is contained in Executive Order 12333, as amended; and procedures issued thereto. The Department of Defense Blanket Routine Uses found at:

http://privacy.defense.gov/blank_et_uses.shtml

apply to this information. Disclosure of requested information is voluntary but refusal to provide requested information may prevent completion of actions to effect this consent form.

CONSENT FORM 3

NSA SIGNALS INTELLIGENCE CONSENT AGREEMENT

I, ____________________________ _______, hereby consent to the National Security Agency or other elements of the United States Signals Intelligence System undertaking to seek and disseminate communications referencing me for the purpose of:

________________________________ ________________________________ ______________

________________________________ ________________________________ ______________

I understand that, unless specified otherwise in the purpose above, communications referencing me may be sought and disseminated while I am in the U.S. during the effective period of my consent. This consent applies to administrative messages alerting elements of the United States Signals Intelligence System to this consent, as well as to any signals intelligence reports that may relate to the purpose stated above.

Except as otherwise provided by law, to include procedures under Executive Order 12333, this consent covers only references to me in foreign communications and information therefrom that relates to the purpose stated above and is effective for the period:

________________________________ _ to ________________________________ _.

Signals intelligence reports containing information derived from foreign communications referencing me may only be disseminated to me and to _____________________________ ___________________, and to others as specified by the U.S. Government as otherwise permitted by law, to include procedures under Executive Order 12333.

________________________________ ___ ______________

Signature Date

________________________________ ___

Title

PRIVACY ACT STATEMENT: Authority for collecting information is contained in Section 6 of the National

Security Agency Act of 1959, Public Law 86-36, codified at 50 U.S.C. 402 note; Executive Order (E.O.) 12333, as amended; and E.O. 13526. NSA's Blanket Routine Uses found at 58 Fed. Reg. 10,531 (1993) and the specific uses found in GNSA 18 apply to this information. Disclosure of requested information is voluntary but refusal to provide requested information may prevent NSA from effecting this consent form.

CONSENT FORM 4

CONSENT AGREEMENT

I, ______________________________ _______, hereby consent to the U.S. Government undertaking to seek and disseminate communications referencing me for the purpose of:

__________________________________ __________________________________ _______________

__________________________________ __________________________________ _______________

I understand that, unless specified otherwise in the purpose above, communications referencing me may be sought and disseminated while I am in the U.S. during the effective period of my consent. This consent applies to administrative messages alerting elements of the U.S. Government to this consent, as well as to any reports that may relate to the purpose stated above.

Except as otherwise provided by law, to include applicable U.S. Government procedures, this consent covers only references to me in foreign communications and information therefrom that relates to the purpose stated above and is effective for the period:

__________________________________ _ to ______________ _____________________.

Reports containing information derived from foreign communications referencing me may only be disseminated to me and to ______________________________ ____________________, and to others as specified by the U.S. government as otherwise permitted by law, to include applicable U.S. Government procedures.

__________________________________ ___ ________________

Signature Date

__________________________________ ___

Title

PRIVACY ACT STATEMENT: Authority for collecting information is contained in Executive Order 12333, as

amended; and procedures issued thereto. The Department of Defense Blanket Routine Uses found at:

http://privacy.defense.gov/blank_et_uses.shtml

apply to this information. Disclosure of requested information is voluntary but refusal to provide requested information may prevent completion of actions to effect this consent form.

USSID SP0018

ANNEX I - (U) FORM FOR CERTIFICATION OF OPENLY ACKNOWLEDGED ENTITIES

SECTION 1 - CERTIFICATION FORM

(U) Certification Form

I1.1. (U) The form below should be used for Director approvals for the collection of communications of entities that are openly acknowledged to be directed and controlled by a foreign power as specified in Section 4 of this USSID.

DIRECTOR, NSA/CHIEF, CSS

Certification for Openly Acknowledged Entities Under
Section 4.A.1.(b) of the Classified Annex
to DOD 5240.1R

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

Certification to the Attorney General:

(~~S//SI//REL~~) The Director, NSA, hereby certifies that [redacted] located in the United States and openly acknowledged to be directed and controlled by (Government X), is a new target of collection. The purpose of the surveillance is (to collect [redacted] intelligence regarding Government X) in accordance with valid intelligence requirements. The surveillance will entail intentional interception or deliberate selection of the target's international communications. Standard minimization procedures will be applied to any information collected that relates to U.S. persons.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

____

Director, NSA/Chief, CSS

Copy to: Deputy Secretary of Defense

USSID SP0018

ANNEX K - (S//REL) [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

SECTION 1 - (U) [redacted]

(b)(3)-P.L. 86-36

(U) [redacted]

K1.1. (U) [redacted]

[redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

(S//SI//REL) [redacted]

[redacted]

Proceed To:
NSA | Director | SIGINT | SIGINT Staff | SIGINT Policy Staff | USSID Index

---

Derived From: NSA/CSSM 1-52
Dated: 8 January 2007
Declassify On: 20360125